Protecting Local Governments from Ransomware Attacks

Kristy James

ABSTRACT

With the rise of global ransomware attacks, managing networks preventing those type of cyber-attacks in local governments can be challenging. Ransomware is defined as a type of malware that attackers use to infect computer networks. Malware is designed to gain unauthorized access to computers or networks and damage or disrupt systems. The ransomware attack can cripple an entire town's network infrastructure without the proper protocols in place. When a ransomware attack occurs, its objective is to encrypt the files, stolen data, from a victim's computer or server. The encrypted data will only be released by the attacker once the victim pays the requested ransom and a decryption key will then be provided. City council members across the country are looking for ways to come together in preparation of going against these attackers. The first big question that is to be answered when or if an attack occurs is whether or not to pay an attackers' demand. Some entities have their own cyber insurance policies in place that would cover the cost of the release of encrypted data, while others have questions about whether or not to buy cyber insurance policies. When speaking to the FBI, they will promptly tell a company or business to never pay a ransom. One of their biggest reasons for this suggestion is seeing historically attackers will share with others in their slimy field of work which companies pay up and then you become a target yet again. Another reason also is the claim that there is never a guarantee the attackers will decrypt the stolen data as well as, the possibilities the attacker could increase their monetary demands. This paper will focus on ways leaders have handled these massive and coordinated attacks that have often been launched from overseas. The findings will be recommended for further review by the government to help protect other local governments from future attacks.

INTRODUCTION

The U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) continues to see a rise in ransomware attacks across the country affecting State and local government entities. Due to this increase, there is a critical need to prioritizing cyber preparations and ensuring networks are secure against attacks. The Multi-State Information Sharing and Analysis Center (MS-ISAC), National Governors Association (NGA), and the National Association of State Chief Information Officers (NASCIO) alongside CISA encourage local government agencies to remain proactive in preventing against ransomware threats (CISA, 2019). This joint effort is recommending agencies regularly backup their systems effective immediately, educate staff and conduct regular training on basic cybersecurity awareness, and establishing a cyber Incident Response Pplan (IRP). Having an IRP in place can help the entity to knowing how to respond or act if a cyber threat affects the organization.

Earlier this month, the Internet Crime Complaint Center (IC3, 2019) announced an alert of ransomware threats to U.S. companies. The cybercriminals in this campaign are targeting organizations through phishing emails to exploit vulnerabilities in Remote Desktop Protocol (RDP), according to the FBI. It has become not just a challenge for the cybercriminal, but instead there is financial gain or incentives to carrying out such attacks. As the criminals become more sophisticated and costly, the frequency of attacks are increasing across the globe. State and local governments are more commonly becoming the visible targets. The FBI does not support paying a ransom due to there being no guarantee the attacker will actually follow through on their promise and release the stolen data. It has been reported in many cases that victims who paid the ransom were never provided the decryption key. The FBI further has explained how the cybercriminals work to make their attack less likely to be detected.

To determine whether or not your organization has become the target of ransomware, it's important to know the difference between encrypted or locked files.

Providing cloud backup solutions can help safeguard specific sensitive data that may not be retained by the cybercriminal. Somewhat often cloud solutions are versioned, meaning snapshots are taken regularly, rendering the data capable of being accessible and roll back on a specific date and time prior to the cyberattack and encryption (Galello, 2019). Also the use of security appliances or software to help protect sensitive data that may offer more than just antivirus protection can provide another solution to protect your network's infrastructure.

The cybercriminals are embedding malicious code into links that are sent via email

phishing campaigns. When the user unknowingly clicks on the link, the malware is then deployed. Businesses are becoming hostage to cybercriminals as they read ransomware threats regularly online or watching the evening news (Mansfield-Devine, 2016). There are several different ransomware attacks that are known to spread through infected email attachments. Some examples of ransomware have been described as very dangerous and different (Kaspersky, 2019).

According to Statista, in a 2018 study, the most targeted types of attacks were through spam, phishing emails, and malicious websites and IT security professionals are feeling the pressure to address each in high numbers (Statista, 2018). Fifteen strains of ransomware were distinguished with managed service providers (MSP) clients. Out of those fifteen, 71-percent indicate CryptoLocker was the top ransomware attack experienced by clients. Having the knowledge to identify vulnerabilities was close behind preventing ransomware attacks. The CryptoLocker is known to search and seize, by encrypting, data files on computers.

CyrptoLocker executables are delivered to the targeted system via email phishing (Abdullahi, 2019). It is an advanced attack that encrypts the data files and locks the system with a ransom note left on the screen demanding payment for decrypted files to be returned.

Petya was discovered in 2016 and would encrypt a victim's entire hard drive. It would begin its vicious spreading via a fake job application appearing to be coming from the HR department. The infected email would point the victim to a Dropbox link. This type of ransomware didn't just encrypt data, but it would also encrypt master boot records (MBR) (Symantec, 2017).

Some cybercriminals are going further and using that victim's email account to spread the infection. There are two different types of ransomware. Both demand that the victims pays a ransom to retrieve their data. The crypto ransomware will encrypt data files and will be released once payment is received, or so is promised by the cybercriminal. Locker ransomware will not encrypt the data; however, it will not be accessible and will lock out to the victim until the demanded ransom is paid.

Ransomware is also being called the crypto-viral extortion technique in which the attacker is using digital currency such as bitcoin which can make it difficult to track the perpetrators. BitCoin is the most commonly used digital currency criminals request in order to pay ransom and receive decrypted data files back (Masarah Paquet-Clouston, 2019).

During a 2001-2018 study, the IC3 reported 2.71 billion U.S. dollars an annual loss of damage caused by cybercriminals (Cybercrime, 2019). The United States has also seen a significant increase in recent months and among those have been attacking databases or SQL files (Clement, 2019). SQL injections is a common attack vector which uses malicious SQL code to manipulate backdoor databases and access sensitive information. Attackers use SQLI vulnerabilities to bypass secure database servers that generally sit behind web applications. According to security magazine 42% of SQL attacks in September decreased (Magazine, 2019). The September 2019 APSAC intelligence report stated there’s a 55% likelihood of a tax by SQL injection (Watson, 2019).

Another common attack vector is Remote Desktop Protocol that is not secured. An RDP exploit allows hackers to sidestep endpoint protection to plant ransomware (Coveware, 2019) by port scanning, brute forcing RDP, and phishing employees to gain access to control their computer and ultimately the organization’s network. Limiting RDP access on a network is vital to one’s integrity and should be disabled for added security unless absolutely necessary. Enabling two-factor authentication (2FA) is another way to secure RDP from ransomware on the network.

Some organizations are opting to purchase cyber insurance; however, when the reputation at the business level has been compromised the loss of trust becomes a bigger issue causing customers to do business elsewhere. Organizations globally are spending $4 billion on cyber insurance. That number is expected to increase closer to $9 billion by the year 2020 (Kshetri, 2018). Recovering from cyberattacks monetarily far exceeds costs associated with natural disasters (France24, 2018). Juniper Research projects cyberattacks will cost organizations $2.1 trillion by the end of 2019 (Research, 2015). Cybersecurity firm, Verisk, predicts cyber liability insurance profits to reach $6.2 billion by 2020 (Group J. , 2018). The increase can be accounted for by organizations requesting additional premiums and larger limits.

Cyber insurance coverage is designed to provide for left or loss of data, as well as expenses related to notifying customers or clients of the data breach, extortion, credit monitoring expenses, and restoring the organization’s reputation through public relations. Ensuring an understanding of what’s covered in the event of a cyber-attack is vital to recovery efforts after any type of cyberattack. Cyber extortion coverage should be broad, but also defined as an explicit threat.

Attaining cyber insurance coverage should be well thought out and can prevent minimal pain or any disruptions in business relations (Raver, 2019). Some items for consideration include:

- Cost effective deductibles to reflect a ransomware event that will not be higher than an actual ransom demand that is paid.
- Research insurers’ reputation regarding whether or not their track record pays for ransomware attack claims or other cyber breaches.
- Maintaining cooperation between cyber insurer, law-enforcement, and other regulatory authorities.
- Securing written consent by the insurer before agreeing to pay ransom. If there is any delay in responding to cyber criminal’s demands, the cybercriminals may increase their request and that puts the extortion coverage into a significantly higher risk.
- Higher level considerations should include extra expenses incurred to keep the organization operational, lost income resulting from the attack, and any type of defense claims or other losses.
- Provide an overview of your current data security systems and policies and procedures.

Like other cyber security professionals, Coveware has been a reporting tool for victims that have been affected by ransomware. Coveware is known as recovery first responders. In one of their reports, Ryuk & Sodinokibi showed a rapid increase in spreading among their clientele during Quarter 2 of 2019. Their findings reported a 184-percent increase in ransom payments made to cybercriminals as compared to Quarter 1 reports (Coveware, 2019). Coveware also reports the average number of days an incident last is 9.6 days.

SophosLabs has recently seen a hike in Ryuk ransomware being delivered in multi-staged attacks, targeting organizations that cannot withstand downtime and ultimately will be easier targets to receive their demanded payments (Adam, 2019). These type of attacks are also carried out via email attachments with malicious code embedded and enables the cybercriminal access to your network. Within your network, the cybercriminals can take over administrative accounts, delete backups, and remove any type of security measures in place before releasing the Ryuk itself, encrypting your data and demanding ransom.

Establishing a firm incident response plan should include identifying threats, ransomware types, risk assessments, securing and safeguard services, and providing all transparent communications. Determining whether or not you should settle with the ransom demand, what the reimbursement cost would be and any if type of professional IT support would need to be provided to include, insurance, documentation on restoring data and posting incident follow up reports.

Symantec discovered the Ransom.Hermes in 2017 which is a Trojan that encrypts data and demands payment for decryption. Symantec encouraged users to follow their best practice recommendations in light of their discovery (Symantec, Ransom.Hermes, 2017).

- Use a firewall to block or deny all incoming connections unless explicitly stated
- Adhere to complex password policy
- Monitor user account control settings
- Disable file sharing
- Turn off and remove unnecessary running services

- Keep systems and software patched and up- to-date
- Isolate compromised systems on network
- Educate and training of employees regularly
- Disable Bluetooth
- Block common spread threats or file attachments, such as .vbs, .bat, .exe, .pif and .scr

A newer strain of ransomware, SamSam, was discovered earlier this year that targets, at the enterprise level, government or healthcare institutions (Zimba, 2019). SamSam enables a worm-like attack on backup systems, ultimately infecting an entire computer network infrastructure. Subsequently, SamSam is more of a spear-phishing vulnerability exploit.

In recent months, the state of Texas Department of Information Resources (DIR) disclosed there were multiple attacks against local government entities (Schwartz, 2019). The Texas Military Department, Texas A&M University System's Cyberresponse and Security Operations Center teams along with Department of Homeland Security and the FBI's cyber division all assisted with the response to the attacks. They did state there were no systems or networks run by the state of Texas directly affected or disrupted any services. The DIR instructed local jurisdictions affected by ransomware attacks to provide the necessary resources to bring the entities back online (TexasDIR, 2019). Some ransomware events are hiding their whereabouts by disguising their identities and location (Manny Fernandez, 2019). The National Security Agency has collected data to help in identifying the sources where the majority have targeted American cities originating from Eastern Europe, the U.S. and Iran. Their view on local government targets is most entities may not have the funds to keep their network infrastructures up to date, backed up, or have the proper cyber security tools in place.

TrendMicro reported through Malwarebytes there was a 363-percent increase in ransomware attacks targeting different public sectors and local government. The use of spam email continues to be a popular distribution of attacking these targets (Ang).

Louisiana school systems were severely impacted by ransomware attacks so the Governor, John Bel Edwards, declared a state of emergency (Mathews, 2019). The declaration assists in obtaining cybersecurity experts and investigations from all across the state of Louisiana to include, the FBI, the state Office of Technology Services, the Louisiana State Police, The Louisiana National Guard, and GOHSEP (Governor's Office of Homeland Security Emergency Preparedness) along with many other agencies.

Local governments are increasingly becoming the target of ransomware attacks in the U.S. (Ferguson, 2019). It has been studied and reported by Recorded Future, that local government ransomware attacks are not always recorded publicly (Liska, 2019). Within this report, 17-percent local government entities paid ransoms demanded by the cybercriminals (Group, 2019). Earlier this year, a Utah county was hit with a ransomware attack that crippled the network for weeks before payment was sent to the cybercriminals. The county attorney stated all their data was taken as a result of someone clicking on a phishing email that launched the attack (Winslow, 2019).

As with other county, state or local governments the FBI and DHS usually will get involved and encourage victims to not pay ransom demands (FBI, 2019). The FBI says there is no guarantee an organization will get all encrypted data returned decrypted and it only encourages the cybercriminal to attempt further attacks.

Some factors causing vulnerabilities are unmanaged devices connected that generally do not have the latest security patches or updates (Supriya, 2018). A lot of these attacks are due to office applications that have been exploited, such as installed applications in the network. An endpoint management solution can help prevent and recover from any type of data breach or attack.

Collectively, more than 225 U.S. mayors are taking a stand against cybercriminals and have signed a resolution proclaiming their stance to not pay ransoms in the event of ransomware attacks or any type of security breach (Lang, 2019). In this resolution, 22 ransomware attacks on city, county and state governments were documented.

The city of Albany in New York announced hackers infected their computers holding them hostage until their demands were paid (NY, 2019). City officials reported their response to the incident last throughout the weekend and provided instructions on obtaining documents or public records that may have been compromised.

During the summer of 2019, Lake City Florida became the first local government to pay hackers in bitcoin to recover its computer systems. Their total bill was over $400,000 (CNET, 2019). Just down the road, Riviera Beach Florida paid hackers $600,000 to retrieve their encrypted data. Each location was derived from an employee clicking on a malicious link (Martin, 2019).

One year after Atlanta's ransomware attack, the city reflects on the incident and its recover efforts (Douglas, 2018). The attack in Atlanta was the worst to ever hit a U.S. city and initially were only requested to pay $51,000 in bitcoin to recover encrypted data files. Ultimately, the city's shortfall has tallied close to $17 million. When Atlanta took this massive cyberattack head on, many devices at City Hall were temporarily halted, approximately five days. Police had to handwrite tickets and incident reports and their in-car video archives became inaccessible. Manually processing cases at the Atlanta Municipal Courthouse and any type of online bill pay or license renewals all became the norm for that temporary pause. Higher impact systems such as online water bill payment systems and the court's online bill pay option returned to service a couple months after the attack.

Throughout Atlanta's recovery efforts, their 911 system and its emergency response, along with major utilities including water and sewer services all continued and operated as usual. Thankfully this was all due to Atlanta having a manual process in place to revert to traditional methods of doing business and maintaining an ongoing operational and continuity assessment.

Center for Internet Security (CIS) provides safeguards to private and public organizations against cyberattacks and threats. CIS is home to Multi-State Information Sharing & Analysis Center (MS-ISAC) which focuses on cyber threat prevention and protection for state, local, tribal and territorial governments. MS-ISAC provides mission critical services as a central resource on cyber threats, such as two-way sharing (CIS, 2019). Organizations can become members and receive 24/7 security operation and incident response services, cybersecurity advisories, access to secure portals and awareness or education materials just to name a few. These services can be beneficial for local governments looking to join a type of cyber alert management program.

The FBI continues its investigation into what virus the Atlanta cyberattack came from. All accounts point to the SamSam family that encrypted portions of their hard drive disks. The city is still slowly restoring and revalidating all their services. Their best recommendations are to segment portions of your network to avoid an entire network infrastructure to go belly-up.

Baltimore City Hall continues to battle its own ransomware attack. With an estimated $8 million gone in lost revenue, their final payment could clear $18 million when all is said and done. Baltimore City's office of Information Technology (BCIT) worked around the clock to reset more than 10,000 employee credentials (Gallagher, 2019). City residents were warned that while the water billing systems were offline, bills would not be able to be generated, so an accumulative cost would be mailed at a later time. Some electronic submissions for parking and camera-generated violations would have to be paid in person and some interactions were being required to mail or hand-deliver paper documents as a temporary workaround. As with previous events, the FBI discouraged Baltimore city from paying the ransom to the cybercriminals. Initially the demand was $70,000. The FBI claims that even if that initial bill is paid, there is never any guarantee of regaining all systems at 100%. Also, going through every system on the network is crucial prior to bringing all back up to ensure the cybercriminals are completely out of your systems. Additional staff would be needed to clean up the mess made and provide forensics to nail down where the attack came from as well as, how it started.

It appeared that the Baltimore mayor had been taunted by the actual cybercriminal behind the ransomware on a now-suspended Twitter account. The Twitter account had a post containing a screenshot of sensitive data and user logins (Kelly, 2019).

Trend Micro reported that Genesse County, Michigan was attacked with ransomware (TrendMicro, 2019). The county IT department isolated the attack and prevent further encryptions, but there was a moment of pause in normal business operations. Within 3 days, the county was able to restore their email services; however, they discovered a setback from their initial observations where their data files were locked.

The Port of San Diego is also recovering from a ransomware attack one year later. They had some public-facing and internal computer systems affected, but would not disclose the type of ransomware used, the amount requested by the cybercriminals, or all the specific information system services affected (Freed, 2018).

Earlier this year, several city services to include the 311 public information hotline, were taken down from a ransomware attack against Akron, Ohio city offices. The hotline was a vital tool used for citizens to access during this time due to a massive snowstorm that simultaneously was affecting the city. Once the cyberattack was discovered, systems were immediately taken offline and the local police were notified (FOH, 2019). Officials stopped taking credit card payments in most local municipalities and resorted to traditionally recording the processing of payments.

The North Carolina water utility, ONWASA, computer systems were taken down by a ransomware attack less than one month from devastating Hurricane Florence that ripped through the area (Olenick). Their systems became infected with Emotet, a Trojan malware program that injects computer code into the network allowing sensitive data to be compromised. After a little more than one week had passed, it was discovered the attack was more of a diversion for the more intrusive attack of systems and data files. The IT department began disconnecting all systems from the network, but the Ryuk ransomware had already began its destruction.

The City of Greenville, NC halted its operations earlier this year after being infected with a new type of ransomware called RobbinHood (Security, 2019). RobbinHood does not contain any self-propagating functions nor does it have any ties to existing malware (Higgins, 2019). It requires another way of spreading instead of machine to machine, by manually planting the ransomware using administrative logins, obtained illegally, and accessing via RDP or domain controller. Deploying on critical systems would create more chaos that will try and disconnect or delete network drives or backups. So it’s more in a sense considered a ransomware-as-a-service than an actual cyberattacker. Different IDs are embedded into templates that have the binary code associated with the RobbinHood attack on both Greenville and Baltimore.

Social engineering has been known to be one of the easiest ways for a hacker to gain access to sensitive information. A cybercriminal can make a simple phone call to a government employee claiming to be someone from their IT department and requesting their password for "testing purposes". Once this information is passed along, that opens up the possibilities of the cybercriminal breaching the network. If the cybercriminal can access the firewall or any other whole in systems, the encryption of data files can begin (Crane, 2019). Other security risks that can leave a network system vulnerable can include lack of spam filtering and not blocking known malicious IP addresses.

As described in many previously discussed ransomware cyberattacks, there are several important steps local governments should take to provide protection against cybercriminals. The FBI and DHS are two of the most important agencies to have on speed dial in the event of such occurrence. The National Governors Association (NGA) provides a State cyber disruption response plan to local and state level municipalities. Public safety and emergency management personnel should be prepared for and know how to respond or recover from any type of cyber disruption (NGA, 2019). The coordination of resources plays a vital role in responding to cyberattacks, as well. The National Cyber Incident Response Plan (NCIRP) is in alignment where it also approaches cyber incidents as significant real world national security threats (CISA, US-CERT, 2019). Federal and state protocols are established in response to "significant cyber incidents".

The state incident response plan relies on seven types of threat schemas detailing and identifying when a plan would be activated.

- Five-level threat schema ranges from "low" to "emergency" with potential impact criteria and procedures for communication.

- Four-level threat schema identifies six incident categories to include: accident, disaster, or computer crimes.
- Three-level threat schema describes what accounts for “minor”, “disaster”, or “major”.
- Risk assessment methodologies are used in conjunction with the notification matrix.

In conclusion, protecting against identified cyber threats is critical in achieving proper security for all levels of municipalities. Understanding at the local government level what is expected to be managed or monitored helps in preparing a response plan in the event of such cyber incident. Being organized and prepared goes a long way when or if the need arises to request assistance from other agencies.

References

(2019). Retrieved from NGA: https://www.nga.org/wp-content/uploads/2019/04/IssueBrief_MG.pdf

Abdullahi, M. M. (2019). An intelligent crypto-locker ransomware detection technique using support vector machine classification and grey wolf optimization algorithms. *I-Manager's Journal on Software Engineering*. doi:doi:http://dx.doi.org/10.26634/jse.13.3.15685

Adam, S. (2019). *Rolling back Ryuk Ransomware.* Retrieved from https://news.sophos.com/en-us/2019/10/04/rolling-back-ryuk-ransomware/

Ang, J. A. (n.d.). Narrowed Sights, Bigger Payoffs: Ransomware in 2019. Retrieved from https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019

CIS. (2019). *Center for Internet Security*. Retrieved from MS-ISAC: https://www.cisecurity.org/ms-isac/

CISA. (2019). *CISA, MS-ISAC, NGA & NASCIO Recommend Immediate Action to Safeguard Against Ransomware Attacks.* US-CERT. Retrieved from https://www.us-cert.gov/sites/default/files/2019-08/CISA_Insights-Ransomware_Outbreak_S508C.pdf

CISA. (2019). *US-CERT.* Retrieved from https://www.us-cert.gov/ncirp

Clement, J. (2019). *Ransomware - Statistics & Facts.* Statista. Retrieved from https://www.statista.com/topics/4136/ransomware/

CNET. (2019). *Another Florida city pays hackers over ransomware attack.* Retrieved from https://www.cnet.com/news/another-florida-city-pays-hackers-over-ransomware-attack/

Coveware. (2019). *Ransomware Amounts Rise 3x in Q2 as Ryuk & Sodinokibi Spread.* Retrieved from https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread

Coveware, R. (2019). *Don’t Become a Ransomware Target - Secure Your RDP Access Responsibly.* Retrieved from https://www.coveware.com/blog/dont-become-a-ransomware-target-secure-rdp

Crane, J. R. (2019). *With ransomware becoming a greater risk, local government agencies doing do what they can to prevent devastating attacks.* Retrieved from https://www.godanriver.com/news/local/with-ransomware-becoming-a-greater-risk-local-government-agencies-doing/article_de1f6a7b-914f-5fed-be68-30f0545805e1.html

Cybercrime. (2019). *Amount of monetary damage caused by reported cyber crime to the IC3 from 2001 to 2018 (in million U.S. dollars).* Statista. Retrieved from https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/

Douglas, T. (2018). *What Can We Learn from Atlanta.* Government Technology. Retrieved from https://www.govtech.com/security/What-Can-We-Learn-from-Atlanta.html

FBI. (2019). On *This Week: Advocating Against Ransomware Payment Demands*. Retrieved from https://www.fbi.gov/audio-repository/ftw-podcast-ransomware-082219.mp3/view

Ferguson, S. (2019). *Ransomware Increasingly Hits State and Local Governments*. Retrieved from https://www.databreachtoday.com/ransomware-increasingly-hits-state-local-governments-a-12481

FOH. (2019). Ransomware attack on Akron, Ohio takes down 311 service amid major snowstorm. *Statescoop*. Retrieved from https://statescoop.com/ransomware-attack-on-akron-ohio-takes-down-311-service-amid-major-snowstorm/

France24. (2018). *France24*. Retrieved from https://www.france24.com/en/20180909-cyber-insurance-market-double-2020-says-munich

Freed, B. (2018). *Port of San Diego recovering from ransomware attack.* Statescoop. Retrieved from https://statescoop.com/port-of-san-diego-recovering-from-ransomware-attack/

Galello, M. (2019). *Not If, But When: Ransomware Attackers Are Targeting Local Governments.* Kronos. Retrieved from https://www.governing.com/topics/workforce/Not-If-But-When-Ransomware-Attackers-Are-Targeting-Local-Governments.html

Gallagher, S. (2019). *ARS Technica*. Retrieved from https://arstechnica.com/information-technology/2019/06/baltimores-bill-for-ransomware-over-18-million-so-far/

Group, C. (2019). *2019 Cyberthreat Defense Report.* Retrieved from https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

Group, J. (2018). *JLT Group*. Retrieved from https://www.jlt.com/en-uk/insurance-risk/cyber-insurance/insights/cyber-insurance-market-grows-as-competition-intensifies

Higgins, K. J. (2019, June). Robbinhood: Inside the Ransomware That Slammed Baltimore. Dark Reading. Retrieved from https://www.darkreading.com/threat-intelligence/robbinhood-inside-the-ransomware-that-slammed-baltimore/d/d-id/1334874

IC3. (2019). *IC3 Issues Alert on Ransomware.*

Kaspersky. (2019). *What are the different types of ransomware?* Retrieved from https://www.kaspersky.com/resource-center/threats/ransomware-examples

Kelly. (2019). *DarkReading*. Retrieved from https://www.darkreading.com/threat-intelligence/baltimore-ransomware-attacker-was-behind-now-suspended-twitter-account-/d/d-id/1334860

Kshetri, N. (2018). The Economics of Cyber-Insurance. *IT Professional*, 9-14. doi:doi: 10.1109/MITP.2018.2874210

Lang, A. (2019). Retrieved from CNET: https://www.cnet.com/news/us-mayors-adopt-resolution-to-not-pay-hackers-over-ransomware-attacks/

Liska, A. (2019). Retrieved from Recorded Future: https://go.recordedfuture.com/hubfs/reports/cta-2019-0510.pdf

Magazine, S. (2019). *Cyberattacks, Application Vulnerabilities Increase by 40 Percent in September 2019*. Retrieved from https://www.securitymagazine.com/articles/91140-cyber-attacks-application-vulnerabilities-increase-by-40-percent-in-september-2019

Manny Fernandez, D. E. (2019). Ransomware Attacks Are Testing Resolve of Cities Across America. *NY Times*. Retrieved from https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html

Mansfield-Devine, S. (2016). Ransomware: Taking businesses hostage. *Network Security*, pp. 8-17. doi:doi:http://dx.doi.org/10.1016/S1353-4858(16)30096-4

Martin, J. (2019). *CNET*. Retrieved from https://www.cnet.com/news/florida-city-will-pay-hackers-600000-to-recover-from-ransomware-attack/

Masarah Paquet-Clouston, B. H. (2019). Ransomware payments in the Bitcoin ecosystem. *Journal of Cybersecurity, 5*(1). doi:https://doi.org/10.1093/cybsec/tyz003

Mathews, L. (2019). Louisiana Governor Declares State of Emergency After Ransomware Hits School Systems. *Forbes*. Retrieved from https://www.forbes.com/sites/leemathews/2019/07/26/louisiana-governor-declares-state-of-emergency-after-ransomware-hits-school-systems/#7d794accb37a

NY, A. (2019). *City of Albany*. Retrieved from https://www.albanyny.gov/newsandevents/pressreleases/19-03-31/City_of_Albany_Outlines_Service_Availability.aspx

Olenick, D. (n.d.). North Carolina water utility ONWASA taken down by ransomware. Retrieved from https://www.scmagazine.com/home/security-news/north-carolina-water-utility-onwasa-taken-down-by-ransomware/

Raver, C. M. (2019). A Ransomware Attack Could Devastate Your Company. Will Your Insurance Cover It? *The National Law Review*. Retrieved from https://www.natlawreview.com/article/ransomware-attack-could-devastate-your-company-will-your-insurance-cover-it

Research, J. (2015). *Juniper Research*. Retrieved from https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion-by-2019

Schwartz, M. J. (2019). Texax Pummeled by Coordinated Ransomware Attack. *Data Breach Today*. Retrieved from https://www.databreachtoday.com/texas-pummeled-by-coordinated-ransomware-attack-a-12926?rf=2019-08-19_ENEWS_ACQ_DBT__Slot1_ART12926&mkt_tok=eyJpIjoiWVRNeE1qVXhaR05qTkRZMyIsInQiOiJySFduN0kwS0FUMVJTTUlNejliS3F2c1Q5eWRKaCtFUTVCYUtxYU9tRGEyWmt2ck5wXC9ZRUMzUFV

Security, P. (2019). RobbinHood: the ransomware that exploits its own reputation. Retrieved from https://www.pandasecurity.com/mediacenter/news/robbinhood-ransomware-notoriety/

Statista. (2018). *Have any of your customers fallen victim to one or more of the following strains of ransomware?* Retrieved from https://www.statista.com/statistics/700944/global-msp-client-ransomware-attack-by-ransomware-families/

Statista. (2018). *Which IT security tasks are you facing the most pressure to address?* Retrieved from https://www.statista.com/statistics/709789/most-pressing-global-cyber-security-issues/

Supriya, R. (2018). Prevention is always better than cure when it comes to cyber security. *Dataquest*. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/2113589198?accountid=10639

Symantec. (2017). *Petya ransomware outbreak: Here's what you need to know.* Symantec Security Response Team. Retrieved from https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper

Symantec. (2017). *Ransom.Hermes.* Retrieved from https://www.symantec.com/security-center/writeup/2017-022015-3241-99

TexasDIR. (2019). *Ransomware Attack Hits Texas Government Entities*. Retrieved from Texas Department of Infromation Resources: https://dir.texas.gov/View-About-DIR/Article-Detail.aspx?id=206

TrendMicro. (2019). Retrieved from https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-attack-hinders-michigan-county-operations

Watson, K. (2019). *September 2019 APPSEC Intelligence Report.* Data Analytics. Retrieved from https://www.contrastsecurity.com/security-influencers/september-2019-appsec-intelligence-report

Winslow, B. (2019, April). Ransomware attack hits Garfield County, shutting off its computer access for weeks. Retrieved from https://fox13now.com/2019/04/11/ransomware-attack-hits-garfield-county-shutting-off-its-computer-access-for-weeks/

Zimba, A. &. (2019). Understanding the evolution of ransomware: Paradigm shifts in attack structures. *International Journal of Computer Network and Information Security*. doi:doi:http://dx.doi.org/10.5815/ijcnis.2019.01.03